

What is claimed is:

1. A method of secure discovery of access nodes in a mobile communication network comprising the steps of:
  - providing a mobile terminal with information identifying a first access node prior to handoff to another access node;
  - after handoff of the mobile terminal to a second access node, receiving at the first access node a message from the second access node requesting verification of information provided by the mobile terminal to the second access node; and
  - verifying the information provided by the mobile terminal to the second access node before updating information on candidate access nodes in the mobile communication network.
2. The method of claim 1 wherein the information on candidate access nodes in the mobile communication network is recorded in a candidate access node table that is shared among mobile terminals in the mobile communication network.
3. The method of claim 1 wherein the information identifying the first access node comprises the network address of the first access node.
4. The method of claim 1 wherein the information provided by the mobile terminal to the second access node comprises a ticket generated by the first access node for the mobile terminal.
5. The method of claim 1 wherein the information provided by the mobile terminal to the second access node is verified by measuring delay occurring during the handoff of the mobile terminal to the second access node.

6. The method of claim 5 wherein timestamps recorded by the first access router and the second access router are utilized to measure the delay occurring during the handoff of the mobile terminal to the second access router.
7. The method of claim 1 wherein the information provided by the mobile terminal to the second access node comprises an identifier for the mobile terminal and wherein the information is verified by checking whether the mobile terminal that provided the information to the second access node is the same mobile terminal that communicated with the first access node prior to handoff.
8. The method of claim 1 wherein the message from the second access node is authenticated.
9. The method of claim 1 wherein a limit is placed on a number of messages received from the mobile terminal prior to verifying the information provided by the mobile terminal to the second access node.
10. The method of claim 1 wherein the mobile terminals are Internet Protocol (IP) devices and wherein the access nodes are IP routers.
11. An access node comprising memory for storing information on candidate access nodes in a mobile communication network and a processor that executes device-readable instructions for performing the steps of:
  - providing a mobile terminal with information identifying the access node prior to handoff to another access node;
  - after handoff of the mobile terminal to a second access node, receiving a message from the second access node requesting verification of information provided by the mobile terminal to the second access node; and
  - verifying the information provided by the mobile terminal to the second access node before updating the information on candidate access nodes in the mobile communication network.

12. The access node of claim 11 wherein the information provided by the mobile terminal to the second access node comprises a ticket generated by the access node for the mobile terminal.
13. The access node of claim 11 wherein the information provided by the mobile terminal to the second access node is verified by measuring delay occurring during the handoff of the mobile terminal to the second access node.
14. The access node of claim 11 wherein the information provided by the mobile terminal to the second access node comprises an identifier for the mobile terminal and wherein the information is verified by checking whether the mobile terminal that provided the information to the second access node is the same mobile terminal that communicated with the access node prior to handoff.
15. The access node of claim 11 wherein the message from the second access node is authenticated.
16. The access node of claim 11 wherein the access node further comprises an Internet Protocol (IP) routing circuit.
17. A mobile terminal comprising memory and a handoff processing circuit that performs the steps of:
  - prior to handoff to another access node, receiving information identifying a first access node and a ticket generated by the first access node;
  - storing the ticket and the information identifying the first access node in the memory;
  - after handoff to a second access node, providing the ticket and the information identifying the first access node to the second access node, so that the second access node can verify the ticket with the first access node prior to updating information on candidate access nodes in the mobile communication network.

18. The mobile terminal of claim 17 wherein the ticket can be utilized by the access nodes to measure delay occurring during the handoff of the mobile terminal to the second access node.

19. The mobile terminal of claim 17 wherein the ticket comprises an identifier for the mobile terminal and wherein the ticket is verified by checking whether the mobile terminal that provided the information to the second access node is the same mobile terminal that communicated with the first access node prior to handoff.

20. The mobile terminal of claim 17 wherein the mobile terminal is an Internet Protocol (IP) device.

21. A method of secure discovery of access nodes in a mobile communication network comprising the steps of:

- receiving from a mobile terminal a candidate access node list associated with and stored at the mobile terminal;

- updating the candidate access node list associated with the mobile terminal to reflect candidate access nodes discovered by the mobile terminal in the mobile communication network; and

- providing the mobile terminal with the updated candidate access list associated with the mobile terminal.

22. The method of claim 21 wherein the candidate access node list is represented as a bitmap whose bits correspond to entries in a candidate access node table.

23. The method of claim 21 wherein the candidate access node list is digitally signed prior to providing the candidate access node list to a mobile terminal.

24. The method of claim 21 further comprising the step of establishing a key for secure message exchange with the mobile terminal before communicating with the mobile terminal.

25. The method of claim 21 wherein the mobile terminals are Internet Protocol (IP) devices and wherein the access nodes are IP routers.

26. An access node comprising memory for storing information on candidate access nodes in a mobile communication network and a processor that executes device-readable instructions for performing the steps of:

receiving from a mobile terminal a candidate access node list associated with and stored at the mobile terminal;

updating the candidate access node list associated with the mobile terminal to reflect candidate access nodes discovered by the mobile terminal in the mobile communication network; and

providing the mobile terminal with the updated candidate access list associated with the mobile terminal.

27. The access node of claim 26 wherein the information on candidate access nodes in the mobile communication network is represented as a candidate access node table and wherein the candidate access node list is represented as a bitmap whose bits correspond to entries in the candidate access node table.

28. The access node of claim 11 wherein the access node further comprises an Internet Protocol (IP) routing circuit.

29. A mobile terminal comprising memory for storing a candidate access node list and a handoff processing circuit that performs the steps of:

providing to an access node in a mobile communication network the candidate access node list associated with the mobile terminal;

receiving from the access node an updated candidate access node list that reflects candidate access nodes discovered by the mobile terminal in the mobile communication network; and

storing the updated candidate access node list in the memory.

30. The mobile terminal of claim 29 wherein the candidate access node list is represented as a bitmap whose bits correspond to entries in a candidate access node table stored in the access node.

31. The mobile terminal of claim 29 wherein the mobile terminal is an Internet Protocol (IP) device.